
VMware VADP Virtualization - Building Block Guide

VMware VADP Virtualization - Building Block Guide

TABLE OF CONTENTS

BACKUP AGENT	SNAPPROTECT BACKUP
Overview Backup Transport Methods Installation Requirements System Requirements Environmental Requirements Port Requirements Change Block Tracking Requirements VDDK Installation User Permission Requirements Backup Permission Requirements Restore Permission Requirements Deployment Scenarios Physical Proxy Computer Installations Hot-Add Installations - Virtualized iDataAgent and Virtualized MediaAgent Hot-Add Installations - Virtualized iDataAgent and Physical MediaAgent Installing the Agent Configuration VADP-Only Configurations Combined VADP and VCB Configurations Configure the Instance, Backup Set, and Subclient Configuration Considerations Master Agent Configurations Backup Restore Container Level Restore File and Folder Level Restore Backup Agent Considerations	SnapProtect Overview SnapProtect User Permission Requirements Backup Permission Requirements Restore Permission Requirements Snapshot Engine Requirements SnapProtect Configuration Enter the Array Information Configure SnapProtect Perform a SnapProtect Backup Perform a SnapProtect Backup Copy Restore Container Level Restore File and Folder Level Restore SnapProtect Considerations

Backup Agent

OVERVIEW

vStorage APIs for Data Protection (VADP) introduces several benefits over the VMware Consolidated Backup (VCB) method of protecting virtual machines. There are several requirements that must be met for VADP to function correctly. This document covers those requirements for both the Virtual Server iDataAgent and VMware infrastructure.

BACKUP TRANSPORT METHODS

The three methods utilized by VADP to transport backup data are defined here.

1. SAN – Data is read directly from the storage where virtual machines reside. This is also referred to as LAN-free since no data is transferred over the network. The LUN(s) containing the virtual machine disks must be visible to the Virtual Server iDataAgent server to support SAN mode backups. SAN mode is supported when utilizing fiber and iSCSI storage.
2. Hot-Add – The Virtual Server iDataAgent is installed on a virtual machine residing on an ESX Server. Hot-Add mode can achieve close to SAN mode performance if SAN is not available. The term Hot-Add refers to the way the backups are completed. In Hot-Add the data volumes containing the virtual machines to be included in the backup are automatically mounted to the virtual machine.
3. NBD & NBDSSL - NBD (network block device) & NBDSSL (encrypted NBD) transmit data over the ESX Servers' TCP/IP connection. This can be the production network or a dedicated backup network.

Refer to the Configuring Transport Modes topic for additional information and instructions on configuring transport modes.

INSTALLATION REQUIREMENTS

SYSTEM REQUIREMENTS

For complete details on the system requirements for VADP environments, see [System Requirements - Virtual Server iDataAgent - VMware](#)

ENVIRONMENTAL REQUIREMENTS

The vCenter server and all ESX Servers should be at vSphere 5.0, 5.1, 4.1 or 4.0 update 2 if possible. Should update 2 on 4.0 not be available, then a common user must be created on the vCenter server and all ESX Servers to avoid vmx file download issues.

- VMware ESX Server Level - ESX(i) servers must be at version 4 or above.
- Disk Types - Independent disks and Physical RDM's are not supported. Virtual RDM's are supported.
- Stand Alone ESXi - Stand-alone ESXi is not supported without the standard license level. License levels are explained in more detail in the following article. <http://blogs.vmware.com/esxi/2009/06/esxi-vs-esx-a-comparison-of-features.html>
- Fault Tolerant virtual machines - Fault Tolerant VMs are not supported for backup.
- Duplicate Disk Names - Virtual machines with duplicate disk names may fail to back up due to a duplicate index entry.
- Duplicate GUID - Virtual machines that have the same GUID may fail on restore.

PORT REQUIREMENTS

Prior to performing any backup or restore operations ensure the port requirements listed below are met.

VIRTUAL CENTER

- Ports for web service (default: 443) and TCP/IP (default: 902) must be opened. Should vCenter be configured to use non-default ports these must be opened.

ESX SERVER

- Ports for web service (default: 443) and TCP/IP (default: 902) must be opened for the vStorage APIs for Data Protection.

CHANGE BLOCK TRACKING REQUIREMENTS

Change Block Tracking (CBT) must be enabled to support VADP backup. The Virtual Server iDataAgent agent will automatically check and enable CBT at the time of backup. Virtual Server iDataAgent may not be able to enable CBT for cloned and migrated virtual machines. CBT can be checked by following the steps documented in the following VMware article: <http://kb.vmware.com/kb/1020128>

VDDK INSTALLATION

The VDDK (Virtual Disk Development Kit) is now pushed with the installation of the Virtual Server iDataAgent. No separate installation is required.

USER PERMISSION REQUIREMENTS

A dedicated account can be used for performing backups on vCenter/ESX Server. The predefined VCB backup role can be copied and modified to perform VADP Backups. This role will require several additional permissions which are listed below. This account only needs to be created in the event that a restricted account is desired.

Restores are typically performed using the admin/root account. However a dedicated account can be created for this purpose. This account requires additional permissions over the account used for backups.

BACKUP PERMISSION REQUIREMENTS

Category	Available Permissions
Datastore	Allocate space Browse datastore Low level file operations
Global	Disable methods Enable methods Licenses
Virtual machine - Configuration	Add existing disk Add new disk Add or remove device Change resource Disk change tracking Disk lease Remove disk Settings

Virtual machine - Provisioning	Allow read-only disk access
	Allow virtual machine download
	Clone virtual machine
Virtual machine - Snapshot management ("Virtual machine - State" in vSphere 4.1)	Create snapshot
	Remove Snapshot

RESTORE PERMISSION REQUIREMENTS

Category	Available Permissions
Datastore	Allocate space
Network	Assign network
Resource	Assign vApp to resource pool
	Assign virtual machine to resource pool
Virtual machine - Configuration	Add existing disk
	Add new disk
	Add or remove device
	Advanced
	Change CPU Count
	Change resource
	Disk change tracking
	Disk lease
	Host USB device
	Memory
	Modify device settings
	Raw device
	Reload from path
	Remove disk
	Rename
	Reset guest information
	Settings
	Swapfile placement
	Upgrade virtual machine compatibility ("Upgrade virtual hardware" in vSphere 4.1)
Virtual machine - Interaction	Power Off
	Power On
Virtual machine - Inventory	Create new
	Register
	Remove
	Unregister
Virtual machine - Provisioning	Allow disk access
	Allow read-only disk access
	Allow virtual machine download
	Mark as template (to restore VM template)
Virtual machine - Snapshot Management ("Virtual machine - State" in vSphere 4.1)	Create snapshot
	Remove Snapshot
	Revert to snapshot

DEPLOYMENT SCENARIOS

The Virtual Server iDataAgent can be installed in several ways to suit environmental needs and resources. Additionally, VADP installations now include VDDK (Virtual Disk Development Kit); no separate installation of this package is required.

The following sections describe frequently used deployment scenarios:

PHYSICAL PROXY COMPUTER INSTALLATIONS

In this configuration, the Virtual Server iDataAgent and MediaAgent are installed on a physical server for SAN only backups with no data transferred over the LAN. A pure physical implementation will often provide the best performance and requires physical hardware with visibility into the storage network.

WHEN TO USE

- Data Stores are configured on FC or iSCSI SAN (No NFS).
- Able to provide Physical Windows server with SAN access to Data Store LUNs
- Direct tape copies are required or physical MAs required for secondary operations.

WHEN NOT TO USE

- SAN access to Data Store LUNs from outside ESX Server environment is not possible.

HOT-ADD INSTALLATIONS - VIRTUALIZED AGENT AND VIRTUALIZED MEDIAAGENT

In this configuration, the Virtual Server iDataAgent and MediaAgent are both installed in Hot-Add mode. The backup destination is typically network based (CIFS/NFS) or another vmfs datastore and tape out options are very limited. Shared storage is required for HotAdd mode backups of virtual machines living on other ESX Server hosts.

WHEN TO USE

- All virtual environment where physical servers are not preferred.
- Data Stores are configured on NFS.
- Each MA can write directly to a mount point presented to the virtual machine
- Able to segregate backup and production traffic on the network.

WHEN NOT TO USE

- Direct backup to tape is required. Backup traffic cannot be segregated from production traffic.

HOT-ADD INSTALLATIONS - VIRTUALIZED AGENT AND PHYSICAL MEDIAAGENT

In this configuration, the Virtual Server iDataAgent is installed in hot-add mode while the MediaAgent is installed on a physical computer. Data is therefore transferred over the LAN to the physical MediaAgent. This model also allows for the use of a centralized and Linux MAs. Shared storage is required for Hot-Add mode backups of virtual machines living on other ESX Server hosts.

WHEN TO USE

- Direct backup to tape or SILO to cloud is required.
- Segregation of backup and production data is possible.
- Physical MA is required for other protection tasks and secondary operations.

WHEN NOT TO USE

- Segregation of backup and production data is not possible.
- SAN based DataStores on FC or iSCSI are in use. (use all physical configuration)

INSTALLING THE AGENT

The Virtual Server iDataAgent can be installed using the steps described in Getting Started - VMware Deployment.

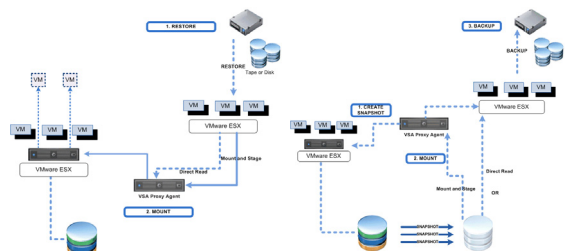
CONFIGURATION

In most environments, the initial configuration of the Virtual Server iDataAgent will include configuring backups of the vCenter. The following sections provide details specific to configurations in VADP environments.

VADP-ONLY CONFIGURATIONS

During backups, the Virtual Server iDataAgent creates a snapshot of the virtual machine data directly from the datastore. The snapshot is then moved directly to the storage media without requiring any dedicated disk cache on the proxy server. In the case of incremental backups, Change Block Tracking (CBT) helps quickly identify the data blocks on the virtual machine that have changed since the last backup.

Similarly, during restores, virtual machines are restored directly to the appropriate ESX Server and datastore without the need for staging on the proxy server with VMware Converter. This capability provides for much faster restores.



COMBINED VADP AND VCB CONFIGURATIONS

You can also perform backup operations from an environment wherein both technologies exist. To accomplish this, simply ensure the following components are

installed on the proxy computer:

- VMware Consolidated Backup (VCB)
- vSphere VADP
- the Virtual Server iDataAgent

Once these components are prepared, backups will leverage between VCB and vSphere as appropriate.

The vStorage API can be used to restore backups performed with VCB. The backup data will first be staged to the proxy and then vStorage will perform the restore.

CONFIGURE THE INSTANCE, BACKUP SET, AND SUBCLIENT

Refer to Getting Started - VMware Configuration complete step-by-step instructions on configuring the Instance, Backup Set, and Subclient.

CONFIGURATION CONSIDERATIONS

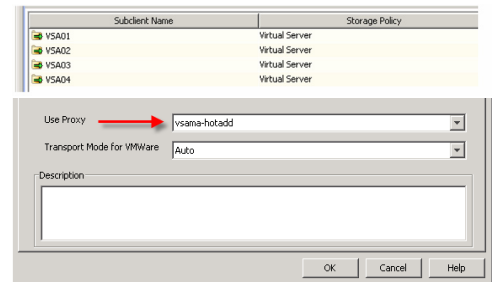
- Regular backups should be performed on the default subclient. This will ensure new virtual machines are discovered on a regular basis along with the backup operation.
- Creating one virtual machine per subclient is not recommended. This creates issues around scheduling and becomes unmanageable in larger environments.
- Typically only the default Subclient will be used in most deployments except in the following cases:
 - Multiple Agents are deployed in the environment and the 'Master' model will be in use. (See the Master Agent Configurations section.)
 - Multiple Storage Policies are required for different virtual machines.
 - Rule-based discovery is in use and different subclients will be used to target a particular affinity.

MASTER AGENT CONFIGURATIONS

When multiple Virtual Server iDataAgents are in use a single Agent can be configured to control and coordinate the activities of all other proxies. This Agent is referred to as the Master Agent and all subclients are created on this client while the actual backup operations are offloaded to other proxies. This will allow all activities to be coordinated from a single interface and reduces the possibility of double backups and/or missed guest machines.

1. Create the subclients on the Master Virtual Server iDataAgent. These can be automatically populated by leveraging one of the automatic discovery options or manually configured.
2. On the General tab of each subclient properties page select the 'Use Proxy' dropdown box and select the desired Virtual Server iDataAgent. Leaving the box blank will default to the proxy the subclient is being created on.

Although the Virtual Server iDataAgent agent needs to be installed on all of the proxies, you should only configure 1 instance on the "master Virtual Server iDataAgent" server. The other proxy machines do not need to have an instance created.

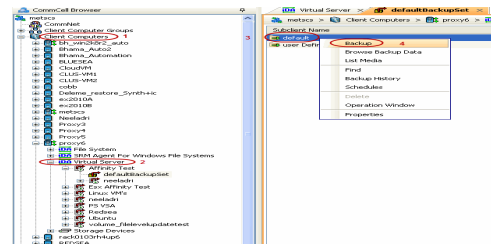


BACKUP

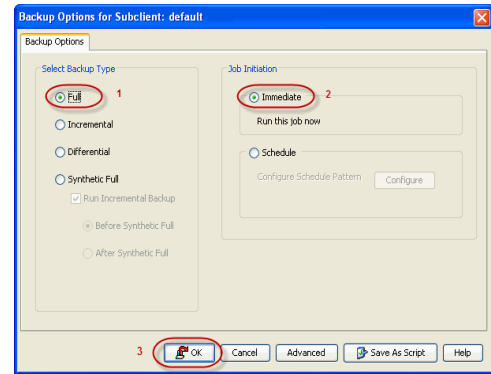
Once the Virtual Server iDataAgent is configured, backup and restore operations are performed as described in Getting Started - VMware Backup.

The following section provides step-by-step instructions for running your first full backup of a single virtual machine immediately.

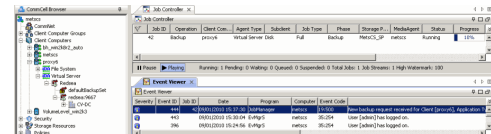
1.
 - From the CommCell Console, navigate to **Client Computers | Virtual Server**.
 - Right-click the **Subclient** and click **Backup**.



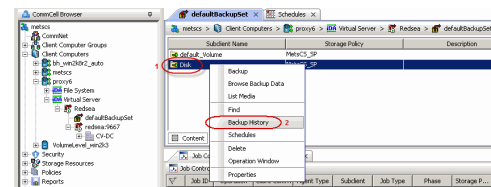
2.
 - Select **Full** as backup type and **Immediate** to run the job immediately.
 - Click **OK**.



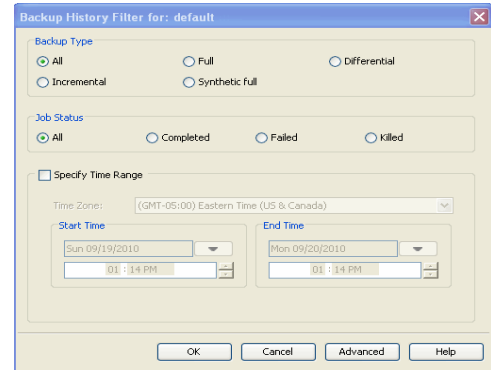
3. You can track the progress of the job from the **Job Controller** window of the CommCell console.



4. Once job is complete, view the details of job from the **Backup History**. Right-click the **Subclient** and select **Backup History**.

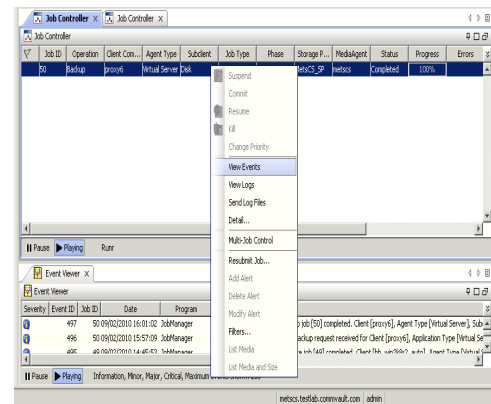


5. Click **OK**.



6. You can view the following details about the job by right-clicking the job:

- Items that failed during the job
- Items that succeeded during the job
- Details of the job
- Events of the job
- Log files of the job
- Media associated with the job



RESTORE

CONTAINER LEVEL RESTORE

A container level restore restores the entire virtual machine disk. Refer to Getting Started - VMware Restore for the steps required to perform this restore following your first full backup.

FILE AND FOLDER LEVEL RESTORE

Files and folders can also be restored from a virtual machine backup. The Advanced - VMware Restore topic includes information on the different restore types available.

BACKUP AGENT CONSIDERATIONS

USING THE VIRTUAL SERVER IDATAAGENT IN HOTADD MODE CONFIGURATIONS

- While deploying the Virtual Server iDataAgent, install the software on a datastore with the largest VMFS block size. This is necessary to ensure that the Virtual Server iDataAgent can mount and back up virtual machines residing on all datastores.
- Helper virtual machines are not required for Hot-Add Virtual Server iDataAgent servers utilizing VADP.

UPGRADING THE VIRTUAL SERVER IDATAAGENT FROM VERSION 8.0.0

VDDK 1.2 is installed to the Base folder with the Virtual Server iDataAgent. Software version 8.0 Virtual Server iDataAgent machines that were upgraded to v9 will need to have the Virtual Disk Development Kit registry key that was manually created during the installation of VDDK 1.1 deleted. Failure to do so will result in the VDDK 1.1 to still be utilized or fail if it has been uninstalled. (VDDK 1.1 does not support HotAdd mode on ESX 4.1)

USING VSTORAGE API

- The vStorage API can be used to restore backups performed with VCB. The backup data will first be staged to the proxy then vStorage will perform the restore.
- Backups performed using the vStorage API cannot be restored through the VMware converter. Converter does not understand the format of vStorage.

CHANGE BLOCK TRACKING

When Change Block Tracking is unavailable backups will revert to CRC to determine changed blocks. Since the Virtual Server iDataAgent needs to read the entire virtual machine disk, CRC incremental backups may take almost as long as full backups. However, the amount of data transferred and stored by an incremental backup is limited to the changed blocks within the virtual disk. Correcting CBT on the problematic virtual machine is recommended as quickly as possible to take full advantage of VADP based incremental backups. Tools are available to check the correct installation of the VDDK and for verifying and correcting CBT issues. Contact your Software Provider for information on these tools.

SUPPORTED VCENTER CONVERTER VERSION

- VMware vCenter Converter Standalone 4.3 no longer supports VCB sources for restores. Version 4.0.1 must be used.
- Fault Tolerant VM's are not supported for snapshot operations and cannot be backed up.

SnapProtect Backup

SNAPPROTECT OVERVIEW

The SnapProtect™ backup enables you to create a point-in-time snapshot of the data to be used for various data protection operations.

SnapProtect backup works in conjunction with software and hardware snapshot engines to provide snapshot functionality for data protection operations. A dedicated ESX Server can be used for selective copy to tier 2 storage. This completely removes any utilization on the ESX Server farm. Granular Recovery can be performed at this stage for individual file and folder recovery.

SNAPPROTECT USER PERMISSION REQUIREMENTS

A dedicated account can be used for performing backups on vCenter/ESX Server. The predefined VCB backup role can be copied and modified to perform VADP Backups. This role will require several additional permissions which are listed below. This account only needs to be created in the event that a restricted account is desired.

Restores are typically performed using the admin/root account. However a dedicated account can be created for this purpose. This account requires additional permissions over the account used for backups.

BACKUP PERMISSION REQUIREMENTS

Category	Available Permissions
Datastore	Allocate space Browse datastore Configure datastore Low level file operations Remove datastore Rename datastore

	Update virtual machine files
Global	Disable methods
	Enable methods
	Licenses
Host - Configuration	Advanced settings
	Connection
	Storage partition configuration
	System Management
Virtual machine - Configuration	Add existing disk
	Add new disk
	Add or remove device
	Change resource
	Disk change tracking
	Disk lease
	Remove disk
Virtual machine - Provisioning	Settings
	Allow read-only disk access
	Allow virtual machine download
Virtual machine - Snapshot Management ("Virtual machine - State" in vSphere 4.1)	Clone virtual machine
	Create snapshot
	Remove Snapshot

RESTORE PERMISSION REQUIREMENTS

Category	Available Permissions
Datastore	Allocate space
	Browse datastore
	Configure datastore
	Remove datastore
	Rename datastore
	Update virtual machine files
Host - Configuration	Advanced settings
	Connection
	Storage partition configuration
	System Management
Network	Assign network
Resource	Assign vApp to resource pool
	Assign virtual machine to resource pool
Virtual machine - Configuration	Add existing disk
	Add new disk
	Add or rRemove device
	Advanced
	Change CPU count
	Change resource
	Disk change tracking
	Disk lease
	Host USB device
	Memory
	Modify device settings
	Raw device
	Reload from path
	Remove disk
	Rename
	Reset guest information

	Settings Swapfile placement Upgrade virtual machine compatibility ("Upgrade virtual hardware " in vSphere 4.1")
Virtual machine - Interaction	Power Off Power On
Virtual machine - Inventory	Create new Register Remove Unregister
Virtual machine - Provisioning	Allow disk access Allow read-only disk access Allow virtual machine download Mark as template (to restore VM template)
Virtual machine - Snapshot Management ("Virtual machine - State" in vSphere 4.1)	Create snapshot Remove Snapshot Revert to snapshot

SNAPSHOT ENGINE REQUIREMENTS

Refer to Storage Arrays Configuration - VMware for information on the requirements and configurations for snap engines.

SNAPPROTECT CONFIGURATION

ENTER THE ARRAY INFORMATION

Refer to Storage Arrays Configuration - VMware for information on the requirements and configurations for snap engines.

Ensure that the array information is entered in the same format that is presented to the ESX server. (for example – should storage be presented by IP to the ESX servers it must also be entered by IP in Array Management)

CONFIGURE SNAPPROTECT

Refer to Getting Started - VMware SnapProtect Configuration for step-by-step instructions on performing the following configuration tasks:

- Configuring the Instance, Backup Set, and Subclient
- Creating a Snapshot Copy
- Configuring the Backup Copy

PERFORM A SNAPPROTECT BACKUP

Refer to Getting Started Backup - Virtual Server iDataAgent (VMware) for step-by-step instructions on performing a SnapProtect Backup.

PERFORM A SNAPPROTECT BACKUP COPY

Refer to Getting Started - Snap Movement to Media for step-by-step instructions on performing a backup copy.

RESTORE

CONTAINER LEVEL RESTORE

A container level restore restores the entire virtual machine disk. Refer to Getting Started - VMware Restore for the steps required to perform this restore following your first full backup.

FILE AND FOLDER LEVEL RESTORE

Files and folders can also be restored from a virtual machine backup. The Advanced - VMware Restore topic includes information on the different restore types available.

SNAPPROTECT CONSIDERATIONS

- It is recommended that the Virtual Server iDataAgent and MediaAgent be installed on a physical computer in environments leveraging fiber channel storage (required for HDS).
- Storage for iSCSI and NFS must be entered in array management in the same format that it is presented to the ESX servers. (i.e. should storage be

connected by IP on the ESX it must entered by IP in Array Management.)

- When leveraging NFS storage an entry for each IP used will need to be entered into the array management. Entering only a single IP for a management interface is not sufficient.
- The Virtual Server iDataAgent proxy must have access to the storage network. If you have an isolated network, an additional network connection must be added to the proxy.
- SnapProtect will perform a full backup. When switching to or from a SnapProtect backup will cause the next backup to be a full backup.

[Back to Top](#)

System Requirements - Virtual Server iDataAgent (VMware)

System Requirements	Supported Features
---------------------	--------------------

The following requirements are for the Virtual Server iDataAgent:

VIRTUAL SERVER APPLICATION SOFTWARE

VMWARE ESX SERVER

VMware ESX/ ESXi 4.x, 5.0, 5.1

vSphere 4.x, 5.0, or 5.1

Before configuring Virtual Server iDataAgent for ESXi servers, consider the following:

- VADP is not available in the free version of ESXi and requires the Essentials licensing level or higher.
- Proxy computers must be running Windows Server 2008 or higher for ESX Server version 5.0 or 5.1.
- VDDK 5.0 is required for this version of ESX server. VDDK 5.0 update 1 is installed automatically with Service pack 6A or higher.

vSphere 5.5 and VDDK 5.5 are supported only in Hitachi Data Protection Suite Version 10. If you need this support, CommVault recommends upgrading to Version 10. You can begin by upgrading the CommServe system, Virtual Server Agent, and MediaAgent, and upgrade the rest of the CommCell environment later.

VMWARE VCENTER SERVER APPLIANCE

VMware vCenter Server Appliance 5.0.0

VIRTUAL MACHINE HARDWARE

Version 4.0, 7.0, 8.0, 9.0

VIRTUAL MACHINE OPERATING SYSTEMS

All Guest Operating Systems supported by VADP and VCB

PROXY COMPUTER OPERATING SYSTEMS

Microsoft Windows Server 2012 R2 is not supported for Hitachi Data Protection Suite Version 9.

Microsoft Windows Server 2012 x64 Edition

Microsoft Windows Server 2008 x64 Edition

Microsoft Windows Server 2003 x64 Edition with a minimum of Service Pack 1

Microsoft Windows 7 x64 Edition

Microsoft Windows Vista x64 Edition

Microsoft Windows XP Professional x64 Edition

VM LIFECYCLE MANAGEMENT

The following conditions must be considered when utilizing VM Lifecycle Management:

- VMware vCenter 4.1 is required
- VMware Tools (version 8288) must be installed on templates
- Windows Server 2008, Windows 7, and Linux (RedHat5) are supported

HARD DRIVE

100 GB recommended.

If performing backups with the granular recovery option enabled, the location of the Job Results folder should contain additional space to accommodate at least 2 percent of the total amount of data being backed up.

MEMORY

1 GB RAM minimum required; 4 GB RAM recommended.

PROCESSOR

All Windows-compatible processors supported

PERIPHERALS

DVD-ROM drive

Network Interface Card

MISCELLANEOUS

ALLOCATION UNIT SIZE OF THE NTFS VOLUMES

The cluster size or the allocation unit size of an NTFS volume in a virtual machine must be multiple of 1024 bytes. You can set the cluster size before formatting a volume. The default cluster size is 4096 bytes.

.NET FRAMEWORK

.NET Framework 2.0 is automatically installed. Note that .NET Framework 2.0 can co-exist with other versions of this software.

MICROSOFT VISUAL C++

Microsoft Visual C++ 2008 Redistributable Package is automatically installed. Note that Visual C++ 2008 Redistributable Package can co-exist with other versions of this software.

NETWORK

TCP/IP Services configured on the computer.

NOTES ON VIRTUAL SERVER iDATAAGENT INSTALLATIONS FOR VMWARE

For VMware, the Virtual Server iDataAgent is installed on a proxy computer that can communicate with the host computer.

Ensure that the VDDK 5.1 is not installed on any host.

SUPPORT FOR VCB ENVIRONMENT

The following utilities must be installed prior to performing any backup operations in the VCB Environment using the Virtual Server iDataAgent (these packages can be obtained from the VMware web site):

- VMware Consolidated Backup (refer to the VMware customer support web site for support information for the VMware Consolidated Backup utility.)
 - The Virtual Server iDataAgent supports all modes supported by the VMware Consolidated Backup utility.
 - Refer to the VMware customer support web site for support information for the VMware Consolidated Backup utility.
- VMware Converter 4.0.1 (refer to the VMware customer support web site for support information for the VMware Converter utility.)
 - Ensure that the guest operating systems are using the supported version of the VMware Converter.
 - The vCenter Converter Standalone 4.0.1 package must be installed for Windows Vista and Windows Server 2008 environments.

Ensure that the latest version of VMware Consolidated Backup and that VMware Converter 4.0.1 are installed.

- Restores of entire virtual machines from ESX Server 4.0 to a prior version of ESX Server are not supported.
- Virtual machines from ESX Server 3.5 can be backed up through vcbmounter, but they are restored through vStorage.

DISCLAIMER

Minor revisions and/or service packs that are released by application and operating system vendors are supported by our software but may not be individually listed in our System Requirements. We will provide information on any known caveat for the revisions and/or service packs. In some cases, these revisions and/or service packs affect the working of our software. Changes to the behavior of our software resulting from an application or operating system revision/service pack may be beyond our control. The older releases of our software may not support the platforms supported in the current release. However, we will make every effort to correct the behavior in the current or future releases when necessary. Please contact your Software Provider for any problem with a specific application or operating system.

Additional considerations regarding minimum requirements and End of Life policies from application and operating system vendors are also applicable